IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:			
	W. Dale Hopkins, et al.	§ Confirmation No.	9964
		§	
Serial No.:	10/749,200	§ Group Art Unit:	2439
		§	
Filed:	December 31, 2003	§ Examiner:	Wang, Harris C.
		§	
For:	PIN VERIFICATION USING CIPHER BLOCK CHAINING	§ Atty Docket:	200309348-1 HPQB:0194
		§	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF TRANSMISSION OR MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted by facsimile to the United States Patent and Trademark Office in accordance with 37 C.F.R. § 1.6(d), or is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.6(a)(4), or is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

September 29, 2010	/Nathan E. Stacy/
Date	Nathan E. Stacy, Reg. No. 52,249

BRIEF IN REPLY TO EXAMINER'S ANSWER DATED JULY 30, 2010

This Reply Brief is being filed in response to the Examiner's Answer dated July 30, 2010. As set forth below, the Appellants respectfully reiterate their request for the Board to review and reverse the Examiner's four grounds of rejection. In the first ground of rejection, the Examiner rejected independent claims 1, 11, 20, and 28-31 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 4,924,514 by Matyas (hereinafter "Matyas") and in view of an IBM Research Report by Coppersmith.

The present application addresses problems of technologies used in verifying cardholder Personal Identification Numbers (PINs). *See* Application, p. 1, l. 10 – p. 2, l. 21 ("Current PIN verification techniques are now known to be cryptographically weak, resulting in a PIN security vulnerability that even exceeds weaknesses in underlying keys

and algorithms. These weaknesses can be attacked by an adversary, potentially resulting in a loss of data security."). The old technique taught by Matyas is specifically mentioned. *See id.* at p. 2, ll. 1-7 and 14-21 ("A difficulty . . . relates to the relationship of the natural PIN, the entered PIN, and the PIN offset. If a PIN is compromised, then an adversary can use the PIN offset to compute a new PIN chosen by the customer."). Ideally, the entered PINs are known to the customer but otherwise secret. *See id.* at p. 1, l. 10 – p. 2, l. 21. A concern with the older verification techniques, such as those taught by Matyas, is that the PIN may be derived by an adversary if the PIN offset is known, even if a new PIN is selected by the customer. Accordingly, the claims provides for input of a second plaintext block, *independent* of the PIN, to the verification cryptography. The dependent claims further provide for: (1) an *irreversible mode* that obstructs recovery of the secret PIN; and (2) *escrow storage* of the second (independent) ciphertext block needed to recover the secret PIN. Thus, advantageously, these features make obtaining or deriving the secret PIN more difficult at the host institution.

Independent claims 1, 11, 20, and 28-31 generally recite a second plaintext block derived from a non-secret entity-identifier *independent* of the PIN, which is not disclosed by Matyas. Instead, Mayas generates an intermediate or natural PIN by encrypting validation data or a PAN, using a PIN generation key (PGK). *See* Matyas, col. 22, ll. 50-54. Thus, if the associated card is reissued with a new PAN, for example, a new intermediate or natural PIN must be generated. Moreover, in Matyas, to allow customer-selectable PINs, a PIN offset value is stored. *See* Matyas, col. 21, ll. 17-29 and 38-42; Fig. 9. The offset is found by subtracting the intermediate or natural PIN from the customer-selected PIN using modulo 10. *See id.* The offset can be stored either on the card track data or in a database at the card issuer, for example. To validate the PIN, the issuing institution calculates the intermediate/natural PIN, adds the offset, and compares the sum to the entered PIN. *See id.* Thus, Matyas does not disclose an input to the cryptographic algorithm independent of the PIN. Yet, the Examiner stated:

> The Natural PIN (the Intermediate PIN of Matyas) is the PAN (Personal Account Number) encrypted with the PGK

> (PIN Generating Key). As the natural PIN is distinct from the customer selected PIN, the cited second input is already independent of the PIN.

Examiner's Answer, pp. 23-24 (emphasis in original) (quoting Final Office Action, p. 2).

However, as understood by the skilled artisan especially in view of the present specification and cited art, while the Matyas algorithmic generated PIN (*i.e.*, an intermediate PIN or natural PIN) may be based on the PAN (personal account number), the Matyas generated PIN is *related* to the customer-selected PIN, such as by an offset/modulo 10. *See* Matyas, col. 21, ll. 17-29 and 38-42; col. 22, ll. 50-54; Fig. 9. Indeed, in the Matyas IBM 3624 system, the *intermediate PIN* referenced by the Examiner *is a function of* the validation data (or PAN), *customer-selected PIN*, and an offset. Plainly, the Matyas intermediate PIN is *not independent* of the customer-selected PIN. Again, as explained in Matyas, and as is typical in the art at the time of Matyas, the intermediate or natural PIN is correlative with the customer-selected PIN via an offset data value (modulo 10). *See id.* Thus, if the offset is known, the customer-selected PIN can be determined from the intermediate or natural PIN. As discussed, a difficulty with this old common relationship of the natural PIN, the entered PIN, and the PIN offset, as taught by Matyas, is that if the PIN is compromised, then an adversary can use the PIN offset to compute a new PIN chosen by the customer. *See* Application, p. 2, ll. 14-21. Thus, selection of a new PIN does not attain security once a PIN is compromised. *See id.*

In sum, the primary reference (Matyas) discloses that a first input to the cryptographic algorithm is the PIN, but a second input is an IBM 3624-formatted PIN algorithmically derived from validation data and which is related to the PIN. *See* Matyas, col. 21, ll. 17-29 and 38-42; col. 22, ll. 50-54; Fig. 9; *see also* Matyas, col. 2, ll. 3-6 and 38-31; col. 4, ll. 26-42; col. 8, ll. 1-18 and 37-42; col. 9, ll. 43-58; Application, p. 2, ll. 1-7 and 14-21. Thus, Matyas results in the difficulties raised by paragraph [0007] in the background section of the present specification. *See* Application, p. 2, ll. 14-21. The

Matyas second input is an intermediate PIN, which is not independent from the customer selected PIN. Further, the secondary references do not remedy these deficiencies.

In addition, with regard to the second and third grounds of rejection, the cited references do not disclose operating in an irreversible mode that obstructs recovery of the secret PIN, as recited in dependent claims 5, 14, and 22. With regard to the fourth ground of rejection, the cited references do not disclose an escrow storage that stores the second ciphertext block to facilitate recovery of the secret PIN, as recited in dependent claims 6, 15, and 23. As explained in the Application:

> [The] PIN verification apparatus 120 operates in an irreversible mode so that, after enrollment, the PIN cannot be recovered by techniques other than an exhaustive PIN search. The irreversible mode may have an option at enrollment to escrow data, enabling recovery of an entity PIN in a secure off-host operation. . .
>
> In irreversible mode . . . the PIN is generally only retrievable by using the ciphertext block C2 escrow.
>
> Selection between reversible and irreversible mode is optional, depending on the security policies of an organization supporting the cards. Some institutions may wish to recover the PIN for various purposes.
>
> *****
>
> . . . a PIN recovery system 510 is shown that can be used to recover a PIN that has been lost or forgotten by a customer. PIN recovery is intended to be a rare operation. The customer PIN is expected to be known only to the customer. The institution that enrolls the customer account and associated magnetic stripe card is generally not to possess the PIN. Therefore, PIN recovery involves communication with the PIN escrow database or databases 504 to supply escrow values in "emergency" conditions.

Application, p. 7, ll. 10-14 and 22-28; p. 11, l.30 – p. 12, l. 10; *see also id.* at p. 11, ll.10-11 ("In the irreversible form, the second ciphertext block C2 can be stored in escrow to facilitate recovery of the secret PIN.").

In contrast, the references do *not* teach an irreversible mode, as claimed. For example, as appreciated by one of ordinary skill in the art, the Matyas IBM 3624 approach (with or without an offset) provides for the issuing entity to generate the customer or secret PIN. Indeed, the techniques taught by the references facilitate local regeneration of the entered PIN, contrary to the instant claims. Further, while the secondary reference (Brachti) discloses the general concept of escrow storage, the combined references do not teach storing a ciphertext block in the escrow storage to *facilitate recovery of the secret PIN*. Lastly, the Appellants respectfully traverse the Examiner's characterization of the claim limitation "to facilitate recovery of the secret PIN" as intended use. Examiner's Answer, p. 26 (contending that the limitation "does not require the recovery of the PIN but only to facilitate recovery."). The recitation "to facilitate recovery of the secret PIN" imparts structural characteristics and limitations to the escrow storage and its coupling/interaction with the recited apparatuses.

Conclusion

The Appellants respectfully submit that all pending claims are in condition for allowance. However, if the Examiner or Board wishes to resolve any other issues by way of a telephone conference, the Examiner or Board is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: September 29, 2010

/Nathan E. Stacy/
Nathan E. Stacy
Reg. No. 52,249
INTERNATIONAL IP LAW GROUP, P.C.
(832) 375-0200

CORRESPONDENCE ADDRESS:
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
Fort Collins, Colorado 80528